Worksheet 18 (Cryptography 2): Transposition Ciphers

Group Names: Solutions

1. The easiest transposition cipher take a plaintext message, arranges it into an array using rows of equal length, padding if necessary, and then uses the columns of the array to form the ciphertext, but it doesn't change the order of the columns.

   Consider the following plaintext:

   THE RIGHT OF THE PEOPLE PEACEABLY TO ASSEMBLE

   (a) Fill in the following grid with the letters of the plaintext (ignores spaces) working across the rows, and then down. The first four letters have been filled in for you.

T	H	E	R	I	G	H	T	
O	F	T	H	E	P	E	O	
P	L	E	P	E	A	C	E	
A	B	L	Y	T	O	A	S	
S	E	M	B	L	E	X	X	

   You will need to fill in blank spaces with "dummy" letters, say X.

   (b) Now construct the ciphertext by writing down the letters in the columns.

   TOPAS HFLBE ETELM RHPYB TEETL GPAOE HECAX TOESX

   (c) Decrypt the phrase O I G R M E R D T E O E A G H E F C B I E D S H R N F O P X assuming it was encrypted using a grid with 5 columns:

   i. There are 30 letters in the phrase. Since we are using 5 columns, how many rows must there be? 6

   ii. Fill in the array down the columns with the ciphertext, and decrypt the message by reading across the rows.

O	R	A	B	R
I	D	G	I	N
G	T	H	E	F
R	E	E	D	O
M	O	F	S	P
E	E	C	H	X

   OR ABRIDGING THE FREEDOM OF SPEECH X

2. Next, we will encrypt a phrase using a **keyword** which tells us how to mix up the rows.

   Consider the following plaintext:

   OR PROHIBITING THE FREE EXERCISE THEREOF

   (a) The plaintext has 35 letters (excluding spaces). How many rows are necessary if there are 6 columns? 6 How many extra letters will be needed? 1

   (b) Write the plaintext in the rows under the key word in the left-hand grid. Add some extra letters to complete the final row.

   (c) Rewrite the letters in the keyword RIGHTS so that they are in order from earliest alphabetically to latest: GHIRST

   (d) Rewrite those letters in the new order on the top row of the right-hand grid, and fill in the corresponding columns from the left-hand grid.

R	I	G	H	T	S
O	R	P	R	O	H
I	B	I	T	I	N
G	T	H	E	F	R
E	E	E	X	E	R
C	I	S	E	T	H
E	R	E	O	F	X

G	H	I	R	S	T
P	R	R	O	H	O
I	T	B	I	N	I
H	E	T	G	R	F
E	X	E	E	R	E
S	E	I	C	H	T
E	O	R	E	X	F

   (e) Now produce your ciphertext by reading down the columns from left to right using the right-hand grid.

PIHESERTEXEORBTEIR OIGECE HNRRHX OIFETF

3. Using the same keyword RIGHTS, undo the previous process to decrypt the following message, which is 36 characters long.

   CEHTUXEBABIXXVSOQXEILNEDSILREXSALERX

   (a) How many rows will you need? ______

   (b) Fill in your sorted keyword on the top row of the right grid and then fill in your ciphertext.

   (c) Then transfer the columns to your left-hand grid and read off the plaintext in the rows.

R	I	G	H	T	S
E	X	C	E	S	S
I	V	E	B	A	I
L	S	H	A	L	L
N	O	T	B	E	R
E	Q	V	I	R	E
D	X	X	X	X	X

G	H	I	R	S	T
C	E	X	E	S	S
E	B	V	I	I	A
H	A	S	L	L	L
T	B	O	N	R	E
V	I	Q	E	E	R
X	X	X	D	X	X

   (d) What is the plaintext?

EXCESSIVE BAIL SHALL NOT BE REQUIRED XXXXX